

THE DISTRIBUTION OF THE NUMBER OF POINTS ON TRIGONAL CURVES OVER \mathbb{F}_q

MELANIE MATCHETT WOOD

ABSTRACT. We give a short determination of the distribution of the number of \mathbb{F}_q -rational points on a random trigonal curve over \mathbb{F}_q , in the limit as the genus of the curve goes to infinity. In particular, the expected number of points is $q + 2 - \frac{1}{q^2+q+1}$, contrasting with recent analogous results for cyclic p -fold covers of \mathbb{P}^1 and plane curves which have an expected number of points of $q + 1$ (by work of Kurlberg, Rudnick, Bucur, David, Feigon and Lalín) and curves which are complete intersections which have an expected number of points $< q + 1$ (by work of Bucur and Kedlaya). We also give a conjecture for the expected number of points on a random n -gonal curve with full S_n monodromy based on function field analogs of Bhargava's heuristics for counting number fields.

1. INTRODUCTION

If we fix a finite field \mathbb{F}_q , we can ask about the distribution of the number of (\mathbb{F}_q -rational) points on a random curve over \mathbb{F}_q . There has been a surge of recent activity on this question including definitive answers of Kurlberg and Rudnick for hyperelliptic curves [11], of Bucur, David, Feigon and Lalín for cyclic p -fold covers of \mathbb{P}^1 [4, 5], of Bucur, David, Feigon and Lalín for plane curves [6], and of Bucur and Kedlaya on curves that are complete intersections in smooth quasiprojective subschemes of \mathbb{P}^n [7]. In the first three cases, the average number of points on a curve in the family is $q + 1$. In contrast, for curves that are complete intersections in \mathbb{P}^n , the average number of points is $< q + 1$, despite, as pointed out by Bucur and Kedlaya, the abundance of \mathbb{F}_q points lying around in \mathbb{P}^n . In this paper, we give the distribution of the number of points on trigonal curves over \mathbb{F}_q (i.e. curves with a degree 3 map to \mathbb{P}^1), and in particular show that the average number of points is greater than $q + 1$.

Let

$T_g := \{\pi : C \rightarrow \mathbb{P}^1 \mid C \text{ is a smooth, geometrically integral, genus } g \text{ curve with } \pi \text{ degree } 3\}$.

Our main theorem is the following.

Theorem 1.1. *Let \mathbb{F}_q have characteristic ≥ 5 . We have*

$$\lim_{g \rightarrow \infty} \frac{\#\{C \in T_g(\mathbb{F}_q) \mid \#C(\mathbb{F}_q) = k\}}{\#T_g(\mathbb{F}_q)} = \text{Prob}(X_1 + \cdots + X_{q+1} = k),$$

where the X_i are independent identically distributed random variables and

$$X_i = \begin{cases} 0 & \text{with probability } \frac{2q^2}{6q^2+6q+6} \\ 1 & \text{with probability } \frac{3q^2+6}{6q^2+6q+6} \\ 2 & \text{with probability } \frac{6q}{6q^2+6q+6} \\ 3 & \text{with probability } \frac{q^2}{6q^2+6q+6}. \end{cases}$$

Moreover, we give a rigorous explanation of the random variables X_i . Theorem 1.1 is a corollary of the following, which gives the distribution of the number of points in the fiber over a given \mathbb{F}_q -rational point of \mathbb{P}^1 .

Theorem 1.2. *Let \mathbb{F}_q have characteristic ≥ 5 . Given a point $z \in \mathbb{P}^1(\mathbb{F}_q)$,*

$$\lim_{g \rightarrow \infty} \frac{\#\{(C, \pi) \in T_g(\mathbb{F}_q) \mid \#|\pi^{-1}(x)(\mathbb{F}_q)| = k\}}{\#|T_g(\mathbb{F}_q)|} = \begin{cases} \frac{2q^2}{6q^2+6q+6} & \text{for } k = 0 \\ \frac{3q^2+6}{6q^2+6q+6} & \text{for } k = 1 \\ \frac{6q}{6q^2+6q+6} & \text{for } k = 2 \\ \frac{q^2}{6q^2+6q+6} & \text{for } k = 3. \end{cases}$$

Moreover, these probabilities (of various size fibers) are independent at the \mathbb{F}_q points z_1, \dots, z_{q+1} of \mathbb{P}^1 .

Corollary 1.3. *The average number of points of a random trigonal curve over \mathbb{F}_q (in the $g \rightarrow \infty$ limit as above) is $q + 2 - \frac{1}{q^2+q+1}$.*

The method used in this paper will be to relate trigonal curves to cubic extensions of function fields, and then to use the work of Datskovsky and Wright [8] to count cubic extensions with every possible fiberwise behavior above each rational point of the base curve. In fact, our methods work with any smooth curve E over \mathbb{F}_q replacing \mathbb{P}^1 . Let $T_{E,g}$ be the moduli space of genus g curves with a specified degree 3 map to E .

Theorem 1.4. *Let \mathbb{F}_q have characteristic ≥ 5 . Given a point $z \in E(\mathbb{F}_q)$,*

$$\lim_{g \rightarrow \infty} \frac{\#\{(C, \pi) \in T_{E,g}(\mathbb{F}_q) \mid \#|\pi^{-1}(x)(\mathbb{F}_q)| = k\}}{\#|T_g(\mathbb{F}_q)|} = \begin{cases} \frac{2q^2}{6q^2+6q+6} & \text{for } k = 0 \\ \frac{3q^2+6}{6q^2+6q+6} & \text{for } k = 1 \\ \frac{6q}{6q^2+6q+6} & \text{for } k = 2 \\ \frac{q^2}{6q^2+6q+6} & \text{for } k = 3. \end{cases}$$

Moreover, these probabilities (of various size fibers) are independent at the \mathbb{F}_q points of E . In particular, the average number of points of a random curve over \mathbb{F}_q with a degree 3 map to E (in the $g \rightarrow \infty$ limit) is $\#|E(\mathbb{F}_q)|(1 + \frac{q}{q^2+q+1})$.

1.1. Related Work. Studying the distribution of the number of points on a curve is equivalent to studying the distribution of the trace of Frobenius on the ℓ -adic cohomology group H^1 . Bucur, David, Feigon and Lalín, for cyclic p -fold covers of \mathbb{P}^1 , in fact give the finer information of the distribution of the trace of Frobenius on each subspace of H^1 invariant under the cyclic action. Their methods, under appropriate interpretation, use Kummer theory to enumerate the cyclic p -fold covers of \mathbb{P}^1 , and thus require the hypothesis that $q \equiv 1 \pmod{p}$. The hardest part of the method is sieving for p -power free polynomials.

The work of Bucur, David, Feigon and Lalín for plane curves [6] and of Bucur and Kedlaya on curves that are complete intersections [7] is also given “fiberwise,” (as in Theorems 1.2 and 1.4 of this paper) in that it computes the probability that any point is the ambient space is in a random smooth curve in the specified family and shows these probabilities are independent. (Here we think of the embedding of a curve $i : C \rightarrow X$, and [6, 7] computes for each point $z \in X(\mathbb{F}_q)$ the distribution of the size of the fiber $i^{-1}(z)$ for random C . Note that since i is an embedding, in this case the fiber has either 0 or 1 points, so these are Bernoulli random variables.)

Kurlberg and Wigman [12] have also studied the distribution of the number of \mathbb{F}_q points in families of curves in which the average number of points is infinite.

In Section 3 of this paper, we discuss distribution of points on other families of n -gonal curves, and in particular give a conjecture for the expected number of points on a random n -gonal curve with full S_n monodromy, based on function field analogs of Bhargava's heuristics for counting number fields. The conjecture in fact predicts the expected number of points in a fixed fiber over \mathbb{P}^1 .

When one instead fixes a genus g and lets q tend to infinity, the philosophy of Katz and Sarnak [10] predicts how the average number of points behaves, and in particular it should be governed by statistics of random matrices in a group depending on the monodromy of the moduli space of curves under consideration.

2. PROOF OF THEOREM 1.4

Let \mathbb{F}_q have characteristic > 3 . Let E be a smooth curve over \mathbb{F}_q , and let k be the function field of E . Then smooth, integral curves over \mathbb{F}_q with finite, degree 3 maps to $\mathbb{P}_{\mathbb{F}_q}^1$ are in one-to-one correspondence with cubic extensions k' of k . However, these smooth, integral curves may not be geometrically integral. In this case, the only such possibility is given by a cubic extension of the constant field of E , and since we will take a $q \rightarrow \infty$ limit, we can ignore this extension altogether.

We now consider all the possible completions of a cubic extension k' of k . For a place v of k , the absolute tame Galois group of the local field k_v is topologically generated by x, y with the relation

$$xyx^{-1} = y^q,$$

where y is a generator of the inertia subgroup and x is a Frobenius element. For a place v of k , the following is a chart of all possible cubic étale k_v algebras L (and thus of all possible isomorphism types for $k' \otimes_k k_v$). To each isomorphism type, we note the images of x, y from the absolute Galois group of k_v in the associated representation to S_3 (given by the action of Galois on the three homomorphisms $L \rightarrow \bar{k}_v$), the number of \mathbb{F}_q rational points in the fiber above v , and a constant c_L that will be important later. (It turns out that $c_L = \frac{1}{|\text{Aut}(L)||D_{L/k_v}|}$, but this fact will not be used.)

L	x	y	# of \mathbb{F}_q points in fiber	c_L
$k_v^{\oplus 3}$	$()$	$()$	3	1/6
$K \oplus k_v, K/k_v$ degree 2 unram. field extn.	(12)	$()$	3	1/2
$K, K/k_v$ degree 3 unram. field extn.	(123)	$()$	0	1/3
$K \oplus k_v, K/k_v$ degree 2 ram. field extn.	$()$	(12)	2	1/2 q
$K \oplus k_v, K/k_v$ degree 2 ram. field extn.	(12)	(12)	2	1/2 q
$K, K/k_v$ degree 3 ram. field extn.	(123)	(123)	1	1/3 q^2 if $q \equiv 1 \pmod{3}$ 0 if $q \equiv 2 \pmod{3}$
$K, K/k_v$ degree 3 ram. field extn.	(132)	(123)	1	1/3 q^2 if $q \equiv 1 \pmod{3}$ 0 if $q \equiv 2 \pmod{3}$
$K, K/k_v$ degree 3 ram. field extn.	$()$	(123)	1	1/3 q^2 if $q \equiv 1 \pmod{3}$ 0 if $q \equiv 2 \pmod{3}$
$K, K/k_v$ degree 3 ram. field extn.	(12)	(123)	1	1/ q^2 if $q \equiv 2 \pmod{3}$ 0 if $q \equiv 1 \pmod{3}$

Let S be the set of places of k corresponding to the \mathbb{F}_q -rational points of E . Let Σ be a choice Σ_v of a cubic étale k_v algebra for each $v \in S$. We define $c_\Sigma = \prod_{v \in S} c_{\Sigma_v}$, where the constants c_{Σ_v} are defined by the chart above. We also choose a Σ' similarly. Let $N_\Sigma(q^{2n})$ be the number of isomorphism classes of cubic extensions k' of k such that for all $v \in S$, we have $k' \otimes_k k_v \cong \Sigma_v$, and such that the norm of the relative discriminant $|D_{k'/k}| = q^{2n}$. Now we can state the result of Datskovsky and Wright and cubic extensions of function fields.

Theorem 2.1 (Corollary of Theorem 4.3 of [8]). *In the above notation*

$$\lim_{n \rightarrow \infty} \frac{N_\Sigma(q^{2n})}{N_{\Sigma'}(q^{2n})} = \frac{c_\Sigma}{c_{\Sigma'}}.$$

Theorem 1.4 now follows because the above chart gives all the possibilities for the completions of cubic extensions k' of k at each \mathbb{F}_q -rational place of k (and the thus determined number of \mathbb{F}_q -rational points in that fiber), and Theorem 2.1 gives their relative probabilities. For a triple cover $(C, \pi) \in T_{E,g}(\mathbb{F}_q)$ corresponding to an extension k'/k , we have $|D_{k'/k}| = q^{2n}$, where $g = n - 1 - \frac{3\chi(E)}{2}$, and thus we can replace the limit in n with a limit in g .

3. FURTHER DIRECTIONS AND CONJECTURES

The above computations of the distribution of points of trigonal curves suggests that similar questions could be attacked for n -fold covers of \mathbb{P}^1 (or an arbitrary curve) using methods from the study of counting extensions of global fields by their discriminants, which

has been more heavily studied in the case of number fields. In analog to this work, one would naturally only study n -gonal curves with a specified monodromy group (i.e. the Galois group of the Galois closure of the field extension). However, for this method to apply, one needs information on the densities of local behaviors of those number fields. In the number field case, such results are only currently available for cubic extensions (the work of Datskovsky and Wright [8] used above, or going back to Davenport and Heilbronn [9] over \mathbb{Q}), for $(\mathbb{Z}/p\mathbb{Z})^k$ Galois extensions ([14, 13]), and for degree n extensions with Galois closure group S_n and $n = 4, 5$ (by work of Bhargava [1, 2]). The first two cases above also have results in the function field case, which have been applied in this paper and forthcoming work of the author, respectively. It is intriguing to ask if a function field version of Bhargava's counting results [1, 2] could give the distribution of the number of points of 4-gonal and 5-gonal curves. In analogy with the number field case, one expects such methods would only count 4-gonal curves with S_4 monodromy, and that D_4 -monodromy curves would be a non-negligible portion of all 4-gonal curves. Since the methods for counting D_4 quartic extensions have not given any results on densities of local behaviors or independence of those behaviors, understanding the distribution of points of 4-gonal curves with D_4 monodromy would be very interesting.

In the case of n -gonal curves with full S_n -monodromy, we can at least predict what the distribution of the number of points in each fiber should be using the heuristics of Bhargava [3, Conjecture 5.1]. In particular, we give the prediction for the average.

Conjecture 3.1. *Let E be a smooth curve over a finite field \mathbb{F}_q of characteristic $> n$ and fix $z \in E(\mathbb{F}_q)$. The average number of points in the fiber over z of a random curve over \mathbb{F}_q with a degree n map to E and full monodromy (in the $g \rightarrow \infty$ limit) is*

$$\frac{\sum_k k \sum_{\ell=0}^{n-1} \frac{p(n, n-\ell, k)}{q^\ell}}{\sum_{\ell=0}^{n-1} \frac{p(n, n-\ell)}{q^\ell}} = 1 + \frac{1}{q} + O\left(\frac{1}{q^2}\right),$$

where $p(n, m, k)$ is the number of partitions of n into m parts such that the parts take exactly k values and $p(n, m)$ is the number of partitions of n into m parts.

It seems within reach to prove this conjecture for $n = 4, 5$ by proving function field analogs of [1, 2]. For $n = 4$ the expected fiber size is (conjecturally)

$$1 + \frac{q^2 + q}{q^3 + q^2 + 2q + 1}$$

and for $n = 5$ the expected fiber size is (conjecturally)

$$1 + \frac{q^3 + 2q^2 + 2q}{q^4 + q^3 + 2q^2 + 2q + 1}.$$

In particular, we now show that Conjecture 3.1 follows from the function field analog of [3, Conjecture 5.1].

Let k be the function field of E and v place of E corresponding to a k_v -rational point. Then [3, Conjecture 5.1]. gives conjectures for local densities for k_v algebras among $k' \otimes_k k_v$ while k' ranges over degree n S_n -extensions of k . In particular, [3, Conjecture 5.1] predicts, as we range over degree n étale k_v algebras L , that L appears with relative density $\frac{1}{|\text{Aut}(L)| |D_{L/k_v}|}$

(recall $|D_{L/k_v}|$ is the absolute norm of the relative discriminant of L/k_v). Recall that isomorphism classes of degree n étale k_v algebras exactly correspond to continuous homomorphisms $\text{Gal}(\bar{k}_v/k_v) \rightarrow S_n$, and we can rephrase the above to say that L appears with relative density

$$\frac{\#\{\chi : \text{Gal}(\bar{k}_v/k_v) \rightarrow S_n \text{ corr. to } L\}}{|D_{L/k_v}|}.$$

Continuous homomorphisms $\text{Gal}(\bar{k}_v/k_v) \rightarrow S_n$ correspond to choices $x, y \in S_n$ such that $xyx^{-1} = y^q$, and $|D_{L/k_v}| = q^{n-\#\text{cycles}(y)}$. The number of \mathbb{F}_q rational points above v in the curve corresponding to the extension k' of k is given by the number of $\langle x, y \rangle$ -orbits on $\{1, \dots, n\}$ that are also $\langle y \rangle$ -orbits.

Let $y \in S_n$ have a_i orbits of size b_i , for $i = 1, \dots, k$. Then the number of $x \in S_n$ such that $xyx^{-1} = y^q$ is $\prod_i a_i! b_i^{a_i}$. If we consider a single cycle σ of y of length b_i , then the number of $x \in S_n$ such that σ remains a $\langle x, y \rangle$ -orbit is $\frac{1}{a_i} \prod_i a_i! b_i^{a_i}$. So given the choice of y , the expected contribution of σ to rational points is $\frac{1}{a_i}$. Thus, given a choice of y , the expected number of rational points is k , the number of distinct cycle lengths of y . Note that $\prod_i a_i! b_i^{a_i}$ is the size of the centralizer of y , so choosing a permutation $y \in S_n$ with relative probability $\frac{\prod_i a_i! b_i^{a_i}}{q^{n-\#\text{cycles}(y)}}$ is the same as choosing it with relative probability $\frac{|\text{Cent}(y)|}{q^{n-\#\text{cycles}(y)}}$ or $\frac{1}{|\text{ConjClass}(y)| q^{n-\#\text{cycles}(y)}}$. This is equivalent to choosing a conjugacy class in S_n , i.e. a partition of n , with relative probability $\frac{1}{q^{n-\#\text{parts}}}$. Since a partition with k distinct part sizes, gives an expected k parts, Conjecture 3.1 follows from the function field analog of [3, Conjecture 5.1].

REFERENCES

- [1] M. Bhargava, The density of discriminants of quartic rings and fields, *Ann. of Math.* (2) **162** (2005), 1031–1063.
- [2] M. Bhargava, The density of discriminants of quintic rings and fields, *Ann. of Math.*, (3) **172** (2010), 1559–1591.
- [3] M. Bhargava, Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants, *Int. Math. Res. Not. IMRN* **2007**, no. 17, Art. ID rnm052, 20 pp.
- [4] A. Bucur, C. David, B. Feigon and M. Lalin, Statistics for traces of cyclic trigonal curves over finite fields, *Int. Math. Res. Not. IMRN*, Advance Access published on October 27, 2009, doi:10.1093/imrn/rnp162.
- [5] A. Bucur, C. David, B. Feigon and M. Lalin, Biased statistics for traces of cyclic p -fold covers over finite fields, to appear in *Proceedings of 2008 Banff Workshop "Women In Numbers"* (in the Fields Institute Communications Series).
- [6] A. Bucur, C. David, B. Feigon and M. Lalin, Fluctuations in the number of points on smooth plane curves over finite fields, *Journal of Number Theory* **130** (2010), 2528–2541.
- [7] A. Bucur, and K. Kedlaya, The probability that a complete intersection is smooth, arXiv:1003.5222v1
- [8] B. Datskovsky and D. J. Wright, The adelic zeta function associated to the space of binary cubic forms. II. Local theory, *J. Reine Angew. Math.* **367** (1986), 27–75.
- [9] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields. II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420.
- [10] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*. American Mathematical Society Colloquium Publications, 45. American Mathematical Society, Providence, RI, 1999. xii+419 pp.
- [11] P. Kurlberg and Z. Rudnick, The fluctuations in the number of points on a hyperelliptic curve over a finite field, *J. Number Theory* **129** (2009), no. 3, 580–587.
- [12] P. Kurlberg and I. Wigman. Gaussian point count statistics for families of curves over a fixed finite field. *Int. Math. Res. Not. IMRN*, to appear.

- [13] M. M. Wood, On the probabilities of local behaviors in abelian field extensions, *Compos. Math.* **146** (2010), no. 1, 102–128.
- [14] D. J. Wright, Distribution of discriminants of abelian extensions, *Proc. London Math. Soc.* (3) **58** (1989), no. 1, 17–50.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, 480 LINCOLN DRIVE, MADISON, WI 53705 USA, AND AMERICAN INSTITUTE OF MATHEMATICS, 360 PORTAGE AVE, PALO ALTO, CA 94306-2244 USA

E-mail address: mmwood@math.wisc.edu